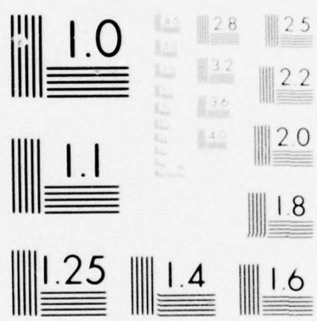
AD-A043 732 CLEMSON UNIV S C DEPT OF MATHEMATICAL SCIENCES F/G 12/1
A LINEAR ALGEBRA PROBLEM OVER FINITE FIELDS.(U)
AUG 77 J V BRAWLEY, J LEVINE N00014-76-C-0130
UNCLASSIFIED TR-257 NL

1 OF 1
AD
A043732

END
DATE
FILMED
9-77
DDC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

DEPARTMENT OF MATHEMATICAL SCIENCES

CLEMSON UNIVERSITY
Clemson, South Carolina

A LINEAR ALGEBRA PROBLEM OVER FINITE FIELDS

J. V. BRAWLEY*

AND

JACK LEVINE

DEPARTMENT OF MATHEMATICAL SCIENCES

CLEMSON UNIVERSITY

TECHNICAL REPORT #257

CONTRACT REPORT N9

*RESEARCH SUPPORTED BY

THE OFFICES OF NAVAL RESEARCH

CONTRACT N00014-76-C-0130

A LINEAR ALGEBRA PROBLEM OVER FINITE FIELDS

by J. V. Brawley* and Jack Levine

ABSTRACT. Let $K = GF(q)$ denote the finite field of order q, let G denote the group of one-to-one maps (permutations) of K onto K, and let $GL(n,K)$ denote the group of $n \times n$ invertible matrices over K. Each triple $(\alpha_1, \alpha_2, A) \in G \times G \times GL(n,K)$ determines a permutation of the vector space K^n of $n \times 1$ matrices over K as follows: $\Pi(X) = \alpha_1^{-1} A \alpha_2(X)$; $X \in K^n$, where α_i acts on X componentwise and A acts on X via matrix multiplication. Two triples (α_1, α_2, A) and (β_1, β_2, B) are called equivalent iff they determine the same permutation Π. This paper determines for a given (α_1, α_2, A) those equivalent (β_1, β_2, B). It turns out that this problem is equivalent to the following one. Given $A \in GL(n,K)$ find all $g_1, g_2 \in G$ such that the mapping $g_1 A g_2^{-1}$ is a linear transformation on K^n. The solution to this latter problem is seen to depend on whether or not A has all row sums equal and whether or not A is a monomial matrix. If A is monomial then the role A plays in the solution depends on the subgroup of $K^* = K - \{0\}$ generated by the set Q of all quotients of nonzero elements of A, and if A is not monomial it depends on the subfield of K generated by Q.

The equivalence relation defined above has its roots in algebraic cryptography where it arises from a question about equivalent cryptosystems based on Hill's method of matrix multiplication.

---

*Research supported in part by O.N.R. Contract N00014-76-C-0130.

Introduction.

Let $K = GF(q)$ denote the finite field of order $q = p^m$, p a prime, let G denote the group of one-to-one maps (permutations) of K onto K, and let $GL(n,K)$ denote the group of $n \times n$ invertible matrices over K. Associate with each triple (α_1, α_2, A) in $G \times G \times GL(n,K)$ a permutation Π of the vector space K^n of $n \times 1$ matrices over K as follows:

$$\Pi(X) = \alpha_1^{-1} A \alpha_2(X); \quad X \in K^n,$$

where α_i is interpreted as acting componentwise on a vector X in K^n and A acts on X via multiplication $X \to AX$. Two triples (α_1, α_2, A) and (β_1, β_2, B) are called equivalent iff they determine the same permutation Π of K^n; i.e., $\alpha_1^{-1} A \alpha_2 = \beta_1^{-1} B \beta_2$, in which case we write $(\alpha_1, \alpha_2, A) \sim (\beta_1, \beta_2, B)$.

The relation $\sim$ while of interest in its own rights has its roots in algebraic cryptography (see below) where it arises from a question concerning equivalence of cryptosystems based on Hill's method [3,4] of matrix multiplication.

The basic problem which we solve in this paper is the following: Given (α_1, α_2, A) find all equivalent (β_1, β_2, B) and determine their number. This problem is readily reformulated (see the next section) into the following problem. Given $A \in GL(n,K)$ find all (g_1, g_2) pairs in $G \times G$ such that $g_1 A g_2^{-1}$ is in $GL(n,K)$ and determine their number.

By way of notation we use K^* to denote the multiplicative group of K. We use $\bar{a}$ to denote the $n \times 1$ matrix in K^n each of whose elements equals $a \in K$. Thus for example, $g(\bar{a}) = \overline{g(a)}$ for every $g \in G$.

The present work is a generalization of previous studies [1,2] which treated the case where $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$ and emphasized the cryptological aspects. Many of the ideas and results of those earlier papers are applicable to the present case. The most striking difference between the two cases is in the changing of the essential role of the matrix A. In [1] and [2] the important features of A were (i) whether or not its row sums were all equal to 1 and (ii) the field and group generated by its nonzero entries a_{ij}. In the present case the important features of A are (i) whether or not A has equal row sums and (ii) the field and group generated by the set of all quotients of nonzero entries from A.

The reader particularly interested in cryptographic interpretations should consult [1, Sections 1 and 2]. The essential idea is briefly described as follows:

Cryptographic Interpretation. Think of the members of K as being the letters of some alphabet, and consider "words" as being members of K^n. Then each (α_1, α_2, A) defines a substitution system which replaces a plain-text word X with a cipher-text word Y using the equation $Y = \alpha_1^{-1} A \alpha_2(X)$. This is essentially the Hill system. In practice in domain K of α_i is actually a set of letters with no algebraic structure and the mapping α_i serves to carry these letters to the finite field K whose

algebraic structure can be utilized. For this reason α_2 is called the <u>plain-text alphabet</u> as it converts plain-text letters to field values and α_1 is called the <u>cipher-text alphabet</u> as α_1^{-1} converts field values to cipher letters.

The Basic Problem.

We now assume (α_1,α_2,A) is given and seek those equivalent (β_1,β_2,B). Since $(\alpha_1,\alpha_2,A) \sim (\beta_1,\beta_2,B)$ iff $\alpha_1^{-1}A\alpha_2 = \beta_1^{-1}B\beta_2$ it follows that $(\alpha_1,\alpha_2,A) \sim (\beta_1,\beta_2,B)$ iff $g_1Ag_2^{-1} = B$ where $g_1 = \beta_1\alpha_1^{-1}$ and $g_2 = \beta_2\alpha_2^{-1}$. Hence we can determine all triples equivalent to the given triple by the following procedure:

(i) Find all $(g_1,g_2) \in G \times G$ such that $g_1Ag_2^{-1}$ is linear; i.e., in $GL(n,K)$

(ii) For each (g_1,g_2) found in (i) put $\beta_1 = g_1\alpha_1$, $\beta_2 = g_2\alpha_2$ and $B = g_1Ag_2^{-1}$.

The collection of all triples (β_1,β_2,B) obtained in this way is precisely the set of triples equivalent to (α_1,α_2,A). Moreover, the number of equivalent triples clearly equals the number of (g_1,g_2) pairs determined in (i). Thus, we can focus our attention on the following problem: Given A characterize those (g_1,g_2) such that $g_1Ag_2^{-1}$ is linear and determine their number. We shall now attack this latter problem.

For convenience, we call a permutation $h \in G$ <u>normalized</u> if $h(0) = 0$ and $h(1) = 1$. We let H denote the subgroup of normalized permutations and define the <u>normalization operator</u> $\psi : G \to H$ by $\psi(g) = h$ where $h(x) = (g(1) = g(0))^{-1}(g(x) - g(0))$. Our next theorem allows us to restrict our search for (g_1,g_2) pairs where $g_1Ag_2^{-1}$ is linear to normalized pairs.

THEOREM 1. *For each* $A \in GL(n,K)$, *let* G_A *and* H_A *be the sets defined by*

(1) $G_A = \{(g_1,g_2) \in G \times G\colon\ g_1Ag_2^{-1}$ *is linear*$\}$

(2) $H_A = \{(h_1,h_2) \in H \times H\colon\ h_1Ah_2^{-1}$ *is linear*$\}$,

and let $\psi : G \times G \to H \times H$ *be the componentwise normalizing operator* $\psi(g_1,g_2) = (\psi(g_1),\psi(g_2))$. *Then* ψ *maps* G_A *onto* H_A. *Moreover, if* A *has constant row sums, all equal to* r, *then the set of* (g_1,g_2) *in* G_A *which map to a given* $(h_1,h_2) \in H_A$ *is precisely the set of* (g_1,g_2) *pairs defined by*

$$(3) \qquad \begin{cases} g_1(x) = m_1h_1(x) + b_2m_1m_2^{-1}h_1(r) \\ g_2(x) = m_2h_2(x) + b_2, \end{cases}$$

where m_1,m_2,b_2 *vary over* K *with* $m_1 \neq 0$, $m_2 \neq 0$. *If* A *does not have constant row sums, the set of* $(g_1,g_2) \in G_A$ *mapping to a given* $(h_1,h_2) \in H_A$ *is precisely the set of* (g_1,g_2) *pairs of the form*

$$(4) \qquad g_1(x) = m_1h_1(x) \quad , \quad g_2(x) = m_2h_2(x),$$

where m_1 *and* m_2 *vary over the nonzero elements of* K.

Proof. Let $(g_1,g_2) \in G_A$ so that $g_1Ag_2^{-1} = B \in GL(n,K)$. Since $g_1A = Bg_2$ it is easily seen from the fact $g_1A\bar{a} = Bg_2(\bar{a})$ for all $a \in K$ that (i) $g_1(\bar{0}) = Bg_2(\bar{0})$ (ii) A has constant row sums iff B has constant row sums, and (iii) if A and B do not have constant row sums $g_1(0) = g_2(0) = 0$. Putting $h_i = \psi(g_i)$,

$i=1,2$ we note that for $X \varepsilon K^n$

$$(5)\qquad \begin{cases} g_i(X) = m_i h(X) + \bar{b}_i \\ g_i h_i^{-1}(X) = m_i X + \bar{b}_i \\ h_i g_i(X) = m_i^{-1}(X-\bar{b}_i) \ , \end{cases}$$

where $m_i = g_i(1) - g_i(0)$, $b_i = g_i(0)$. It follows that $h_1 A h_1^{-1}(X) = h_1 g_1^{-1} g_1 A g_2^{-1} g_2 h_2^{-1}(X) = h_1 g_1^{-1} B g_2 h_2^{-1}(X) = h_1 g_1^{-1}(B(m_2 X+\bar{b}_2) = m_1^{-1}(m_2 BX+B\bar{b}_2-\bar{b}_1) = m_1^{-1} m_2 BX$; hence $(h_1,h_2) \varepsilon H_A$. If A has unequal row sums we note that $b_i = g_i(0) = 0$ implying g_i has the form (4). If A has all row sums equal to r, we note that $h_1 A h_2^{-1}(\bar{1}) = m_1^{-1} m_2 B(\bar{1})$ implies $h(r) = m_1^{-1} m_2 r_B$ where r_B is the row sum of any row of B; thus, since $g_1(\bar{0}) = Bg_2(\bar{0})$ we see that $b_1 = r_B b_2 = m_2^{-1} m_1 h(r) b_2$ showing that g_1 and g_2 have the form (3).

Finally, let $(h_1,h_2) \varepsilon H_A$; i.e., $h_1 A h_2^{-1} = C \varepsilon GL(n,K)$, If A has constant row sums r then so does C and $h_1(r) = r_C$; thus if g_1 and g_2 are any two permutations defined by (3) then equations (5) are valid and $g_1 A g_2^{-1}(X) = g_1 h_1^{-1} h_1 A h_2^{-1} h_2 g_2^{-1}(X) = g_1 h_1^{-1} C h_2 g_2^{-1}(X) = g_1 h_1^{-1}(C(m_2^{-1}(X-\bar{b}_2))) = m_1 m_2^{-1} CX - m_1 m_2^{-1} C\bar{b}_2 + \bar{b}_1 = m_1 m_2^{-1} CX - m_1 m_2^{-1} h(r)\bar{b}_2 + b_1 = m_1 m_2^{-1} CX$. Thus $(g_1,g_2) \varepsilon G_A$. A similar argument is valid when A does not have constant row sums so the proof is complete.

COROLLARY 1.1. Let $A \varepsilon GL(n,K)$. Then

$$(6)\qquad |G_A| = \begin{cases} q(q-1)^2|H_A|; & \underline{\text{if}}\ A\ \underline{\text{has}}\ \underline{\text{constant}}\ \underline{\text{row}}\ \underline{\text{sums}} \\ (q-1)^2|H_A|; & \underline{\text{otherwise}}. \end{cases}$$

COROLLARY 1.2. *Let* $A \in GL(n,K)$ *and let* $(h_1,h_2) \in H_A$. *If* g_1 *and* g_2 *are defined by* (3) *or* (4) *according as* A *does or does not have constant row sums, then*

$$h_1Ah_2^{-1} = (h_1(a_{ij})) = h_1(A).$$

and

$$g_1Ag_2^{-1} = m_1m_2^{-1}h_1(A).$$

Proof. Put $C = h_1Ah_2^{-1}$. We need only show that $C = (h_1(a_{ij}))$. Letting U_j, C_j, and A_j denote respectively the jth columns of I (identity matrix), C and A we have $C_j = CU_j = h_1Ah_2^{-1}U_j = h_1(AU_j) = h_1(A_j)$; thus, $c_{ij} = h_1(a_{ij})$.

Since it is now clear how to obtain G_A sets from H_A sets we now attack the problem of finding H_A given A.

Recall that A is *monomial* iff A has exactly one nonzero entry in each row and column. The set of monomial matrices denoted by M is a subgroup of $GL(n,K)$. It will be convenient to treat separately the case $A \notin M$ and $A \in M$.

THEOREM 2. *Let* $A \in GL(n,K) - M = M'$, *let* Q *denote the subfield of* K *generated by the set of all quotients* a/b *where* a,b *are nonzero entries in* A, *and let* h_1,h_2 *be normalized permutations of* K. *The mapping* $h_1Ah_2^{-1}$ *is linear if and only if for all entries* a_{ij} *of* A, *for all* $x,y \in K$ *and for all* $c \in Q$

we have

$$(7) \quad h_1(x+y) = h_1(x)+h_1(y)$$

$$(8) \quad h_1(cx) = h_1(c)h_1(x)$$

$$(9) \quad h_1(a_{ij}x) = h_1(a_{ij})h_2(x).$$

Proof. Suppose first that h_1 and h_2 satisfy conditions (7) and (9) of the Theorem. Putting $C = h_1(A) = (h_1(a_{ij}))$ we have $Ch_2X = (\sum_j c_{ij}h_2(x_j)) = (\sum h_1(a_{ij})h_2(x_j)) = (\sum h_1(a_{ij}X_j)) = (h_1(\sum a_{ij}x_j)) = h_1AX$. Thus $h_1Ah_2^{-1} = C$ is linear.

Now suppose $h_1Ah_2^{-1} = C$ is linear. Then $h_1A = Ch_2$ where $C = h_1(A)$ (by COROLLARY 1.2). Let U_j and U_k be the jth and kth unit vectors, and let $x,y \in K$. Then $h_1A(xU_j+yU_k) = h_1(A)h_2(xU_j+yU_R)$ so that $h_1(a_{ij}x+b_{ik}y) = h_1(a_{ij})h_2(x) + h_1(b_{ik})h_2(y)$. Taking $y = 0$ we obtain condition (9), and using this condition we have further that $h_1(a_{ij})h_2(x) + h_1(b_{ij})h_2(y) = h_1(a_{ij}x) + h_1(b_{ij}y)$. Since some row of A has two nonzero entries we have $h(ax+by) = h(ax) + h(by)$ for $a,b \neq 0$. Take $x = a^{-1}x'$ and $y = b^{-1}y'$ to obtain $h_1(x'+y') = h_1(x') + h_1(y')$ so condition (7) is valid. We complete the proof by showing (7) and (9) imply (8). Let $c = a/b$ denote a quotient of two nonzero entries a,b from A. From (9) we have $h_1(ax)/h_1(a) = h_1(bx)/h_1(b)$; hence, putting $x = y/b$ we obtain $h_1(cy) = h_1(a)h_1(y)/h_1(b)$. Taking $y=1$ shows that $h_1(c) = h_1(a)/h_1(b)$; hence, $h_1(cy) = h_1(c)h_1(y)$. Now it is readily argued that the set defined by $S = \{s \in K : h_1(sx) = h_1(s)h_1(x)\}$ is a subfield of K, and since S contains $c = a/b$

it contains Q. Thus (8) is valid.

It should be noted that the field Q generated by the quotients of elements from A is a subfield of the field generated by the elements of A. It should also be noted that THEOREM 2 implies h_2 is uniquely determined by h_1. The next theorem shows that any $h_1 \in H$ satisfying (7) and (8) can be used to construct an h_2 where $(h_1 h_2) \in H_A$.

THEOREM 3. _Let_ A _and_ Q _be as in_ THEOREM 2, let $h_1 \in H$ _satisfy_ (7) _and_ (8), _and let_ a _be a nonzero entry in_ A. _Then the mapping_ h_2 _defined by_

$$h_2(x) = (h_1(a))^{-1}(h_1(ax)$$

_is in_ H _and is independent of the choice of_ A.

Proof. Clearly $h_2 \in H$; thus let a_{ij} be an arbitrary nonzero entry in A and put $c = a_{ij}a^{-1} \in Q$. Since $h_1(a_{ij}) = h_1(a_{ij}a^{-1}a) = h_1(ca) = h_1(c)h_1(a)$ it follows that $h_1(c) = (h_1(a_{ij})(h_1(a))^{-1}$; thus, $h_1(a_{ij}x) = h_1(cax) = h_1(c)h_1(ax) = h_1(a_{ij})(h_1(a))^{-1}h_1(ax)$. Hence, $h_2(x) = (h_1(a))^{-1}h_1(ax) = (h_1(a_{ij}))^{-1}h_1(a_{ij}x)$ and the proof is complete.

In [1,p.127,THEOREM 4.2] the authors give an explicit description of those functions $h \in H$ satisfying (7) and (8) for a given subfield $Q = GF(p^t)$ of $K = GF(p^m)$. In particular it is shown that h satisfies (7) and (8) iff h has the form

$$h(x) = \sum_{i=1} \sigma(a_i)w_i$$

where $d = [K:Q] = m/t$, $\langle 1, w_1, w_2, \ldots, w_d \rangle$ is an arbitrary ordered basis for K over Q, and $a_1, \ldots, a_d \in Q$ are the coordinates of x with respect to a fixed ordered basis $\langle 1, v_2, \ldots, v_d \rangle$ of K over Q. Moreover, the number of such h functions is shown to be

$$N_1(m,t) = t \prod_{i=1}^{d} (p^m - p^{it}). \tag{10}$$

Putting all of these ingredients together it is now clear how to find for a given nonmonomial matrix A all (g_1, g_2) pairs such that $g_1 A g_2^{-1}$ is linear. This procedure is summarized below after we indicate how to proceed in case A is monomial.

THEOREM 4. *Let $A \in M$ and let R denote the subgroup of K^* generated by all quotients of the nonzero entries of A. Then $(h_1, h_2) \in H \times H$ is in H_A iff for all $x \in K$, $c \in R$ and nonzero entries a of A we have*

$$h_1(cx) = h_1(c)h_1(x) \tag{11}$$

$$h_1(ax) = h_1(a)h_2(x). \tag{12}$$

THEOREM 5. *Let A and R be as in THEOREM 4, let h_1 satisfy (11), and let a be a nonzero entry in A. Then the map h_2 defined by*

$$h_2(x) = h_1(ax)/h_1(a)$$

is in H and is independent of the choice of a.

The proofs here are similar to those above and will be omitted. Note again that (12) implies h_2 is uniquely determined by h_1. The functions $h_1 \in G$ satisfying (11) have been described in [1,p.131,THEOREM 5.2]. The number of such functions is shown to be

$$(13) \qquad N_2(m,r) = (e-1)!r^{e-1}\phi(r)$$

where $r = |R|$ and $e = (p^m-1)/r$, and ϕ is the Euler ϕ-function.

A procedure for finding those (β_1,β_2,B) triples equivalent to a given (α_1,α_2,A) as well as a procedure for finding H_A and G_A given A is described as follows:

1. If $A \not\in M$ (respectively $A \in M$) determine the subfield $Q = GF(p^t)$ of K (subgroup R of K^*) generated by the set of quotients of nonzero elements of A.

2. Determine the mappings h_1 satisfying (7) and (8) (respectively (11)). The number of such mappings is given by (10) (respectively (13)).

3. Pick an arbitrary nonzero entry a in A and for each h_1 found in step 2 determine h_2 by $h_2(x) = h_1(ax)/h_1(a)$. The pairs thus obtained are the members of H_A. Here $h_1Ah_2^{-1} = h_1(A)$, and $|H_A| = N_1(m,t)$ (respectively, $N_2(m,r)$, $r = |R|$).

4. Construct the set G_A by obtaining for each (h_1h_2) pair the corresponding (g_1,g_2) pairs described in THEOREM 1. Here $g_1Ag_2^{-1} = m_2^{-1}m_1h_1(A)$ where $m_1 = g_1(1) - g_1(0)$, $m_2 = g_2(1) - g_2(0)$. The number of such pairs is given by COROLLARY 1.1 together with

the above formula for $|H_A|$.

5. For each $(g_1, g_2) \in G_A$ determine (β_1, β_2, B) by $\beta_1 = g_1\alpha_1$, $\beta_2 = g_2\alpha_2$, $B = m_2^{-1} m_1 h_1(A)$. The number of such triples is $|G_A|$.

Using techniques similar to those in [2] one can now find the number of equivalence classes of the relation $\sim$ but this will not be developed here.

References.

1. Brawley, J. V. and Jack Levine. Equivalence classes of linear mappings with applications to algebraic cryptography, I, Duke Math. J. 39(1972):121-132.

2. Brawley, J. V. and Jack Levine. Equivalence classes of linear mappings with applications to algebraic cryptography, II, Duke Math. J. 39(1972):133-142.

3. Hill, Lester S. Cryptography in an algebraic alphabet, Amer. Math. Monthly, 36(1929):306-312.

4. Hill, Lester S. Concerning certain linear transformation apparatus of cryptography. Amer. Math. Monthly, 38(1931): 135-154.

Unlimited
Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)

Department of Mathematical Sciences
Clemson University
Clemson, South Carolina

2a. REPORT SECURITY CLASSIFICATION: Unclassified

2b. GROUP

3. REPORT TITLE

A Linear Algebra Problem Over Finite Fields.

9 Technical repts

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

14 TR-257, CR-N9

5. AUTHOR(S) (First name, middle initial, last name)

J. V. Brawley and Jack Levine

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
8/1/77 11 1 Aug 77	14	4

8a. CONTRACT OR GRANT NO.: N00014-76-C-0130

b. PROJECT NO.

c.

d.

9a. ORIGINATOR'S REPORT NUMBER(S): N9

12 17p.

9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. DISTRIBUTION STATEMENT

Unlimited

alpha(1) inverse A alpha(2)

11. SUPPLEMENTARY NOTES

element of

12. SPONSORING MILITARY ACTIVITY

alpha

elements of

407 183

13. ABSTRACT

Let K = GF(q) denote the finite field of order q, let G denote the group of one-to-one maps (permutations) of K onto K, and let GL(n,K) denote the group of $n \times n$ invertible matrices over K. Each triple $(\alpha_1, \alpha_2, A) \in G \times G \times GL(n,K)$ determines a permutation of the vector space K^n, of $n \times 1$ matrices over K as follows: $\Pi(X) = \alpha_1^{-1} A \alpha_2(X)$; $X \in K^n$, where α_i acts on X componentwise and A acts on X via matrix multiplication. Two triples (α_1, α_2, A) and (β_1, β_2, B) are called equivalent iff they determine the same permutation Π. This paper determines for a given (α_1, α_2, A) those equivalent (β_1, β_2, B). It turns out that this problem is equivalent to the following one. Given $A \in GL(n,K)$ find all $g_1, g_2 \in G$ such that the mapping $g_1 A g_2^{-1}$ is a linear transformation on K^n. The solution to this latter problem is seen to depend on whether A has all row sums equal and whether or not A is a monomial matrix. Moreover, if Q is the set of all quotients of the nonzero entries of A then the role A plays in the solution is a function of either the subfield of K or the subgroup of $K^* = K - \{0\}$ generated by Q.

The equivalence relation defined above has its roots in algebraic cryptography where it arises from a question about eqivalent cryptosystems based on Hill's method of matrix multiplication.

super n beta alpha

DD FORM 1473 1 NOV 65 (PAGE 1) PLATE NO. 21856

S/N 0102-014-6600

Unclassified
Security Classification

6pg